The President's National Security Telecommunications Advisory Committee

R&D Exchange
Physical Breakout Session

Mr. David Barron, BellSouth
Mr. Jim Craft, Raytheon

March 14, 2003

Physical: Current State of Trustworthiness

The current state of trustworthiness related to the physical security of telecommunications assets is characterized by:

- No defined or government validated threats or adversary attack plan against which to protect facilities
- Inability to protect against all feasible attack techniques
- Difficulty in determining what threats exist with regard to the telecommunications industry
- Lack of widespread understanding and appreciation of the sophistication of threats
- Lack of procedures for protecting companies' human capital during times of attack (need to focus on people not just physical assets)

Physical: Priorities

Members of the physical breakout session defined the following top priorities for further investigation through industry/government partnership(s):

- Undertake simulation for NS/EP events and modeling that includes virtual attack/defense of facilities/networks
- Develop better vulnerability analysis to understand critical single points of failure and interdependencies
- Develop industry standards for and implement a national standard industrial I.D. card that is biometrics based
- Investigate standards for the diversity of critical infrastructure
- Develop a system for the automatic defense of cable routes from “backhoes”, etc
- Provide better background checks for people with access to critical facilities
- Develop a process to analyze patterns of facility use (looking for social engineering, data mining, etc)
- Withdraw critical vulnerability information from the public domain

Physical: Technology To Improve Trustworthiness

- “Sim Facility” Simulation (like SimCity Game)
- Modeling that includes virtual attack/defense of facilities/networks
- Modeling of cascading, cross sector and widespread/catastrophic outages
- Biometrics
- Immune building technology to deal with biohazards

Physical: Impediments to Future R&D on Trustworthiness

- **Financial constraints**
  - **Companies/Governments do not have the financial/human resources to protect against every possibility**
  - **Regulatory and other pressures may limit some security investments**
- **Competitive nature of the telecommunications industry**
- **Information sharing**
  - **Making information available to the parties that need it without increasing vulnerabilities**
  - **Government does not explain its need and projected use of highly sensitive industry data**
    - **Industry and Government do not demonstrate mutual trust**

Physical: Agenda for Action

An Agenda for Action should:

- Define levels of "critical" and determine what telecommunications assets can be considered critical for NS/EP purposes and interdependencies
- Determine what threats exist with regard to the telecommunications industry and develop a rapid method for disseminating this information to those in industry who need it
- Develop modeling and simulations technology related to protection of those assets deemed critical